International Journal of Innovative
Computing, Information and Control
Volume **8**, Number **11**, November **2012**

 ISSN 1349-4198
pp. **7943–7953**

AN EFFICIENT SEALED-BID AUCTION PROTOCOL WITH BID PRIVACY AND BIDDER PRIVACY

Wenbo Shi

Department of Electronic Engineering
Northeastern University at Qinhuangdao
No. 143, Taishan Road, HaiGang District, Qinhuangdao 066004, P. R. China
swb319@hotmail.com

Received July 2011; revised December 2011

Abstract. *In this paper, a sealed-bid auction protocol which mainly focuses on security issues: bid privacy, bidder anonymity and fairness problem is presented. The new proposal is motivated by the conflict between bidder anonymity and DOS (denial-of-service) attack from insider. It utilizes an efficient LPN-based authentication method to accomplish lightweight authentication. In order to share the determination process data, the market constructs a simple interpolating polynomial to those suppliers who participated in this auction. Sharing the determination process data can totally avoid collusion between a customer and a certain supplier and achieve public verifiability. Also, the proposed scheme relaxes the trust assumptions for three-party. According to comparison and analysis with other protocols, the proposed protocol requires less computation cost.*
Keywords: Electronic auctions, Anonymity, Cryptography, Ticket token, Learning Parity with Noise (LPN)

1. **Introduction.** Electronic commerce has become more and more important along with the growth of the Internet. In particular, Internet auctions have become a powerful engine of electronic commerce and have been implemented in many domains with assorted environments. Online Auctions can be roughly classified into open-bid auctions and sealed-bid auctions. In open-bid auctions, bidders know the bid value of other bidders. In sealed auctions, the participants' bids are not disclosed to others [1]. On the other hand, auction protocols can be classified into two types: one-sided auction and two-sided auction. A single seller (or buyer) accepts bids from multiple buyers (or seller) in one-sided auction protocols, and multiple buyers and sellers are permitted to bid/ask for designated goods in two-sided or double auction protocols [2,3].

For one-sided auctions, there are examples such as English auction, Dutch Auction, First-price Auction, Second-price Auction and Sealed-bid auction [1-4]. In the English auction, each bidder is free to raise his/her bid. When no bidder is willing to raise anymore, the auction ends, and the highest bidder wins the item at the price of his/her bid. In the first-price sealed-bid auction, each bidder submits one bid without knowing the others bids. The highest bidder wins the item and pays the amount of his/her bid. In the Dutch (descending) auction, the seller continuously reduces the price until one of the bidders takes the item at the current price. In the Second-price Auction (Vickrey) auction, each bidder submits a bid without knowing the others bids. The highest bidder wins, but at the price of the second highest bid.

Security issue is one of the main issues of online auction protocol. Researchers have defined security requirements and studied how to solve various security problem [4-7].

Firstly, this study follows OMOTE et al.' security requirements to introduce some auction properties [4-7].

(1) Anonymity: no one should be able to identify the bidder during the auction. (2) Traceability: the winning bidder must be identifiable at the end of the auction. (3) No framing: no one shall participate in the auction as the identity of another bidder. (4) Unforgeability: no one shall falsify a valid bidding price. (5) Non-repudiation: bidders cannot deny their bid after the winning bidder has been announced. (6) Fairness: bidding must be justly handled by the auction manager. (7) Public verifiability: anyone can confirm the identities of bidders and the validity of their bids. (8) Unlinkability (among different rounds of an auction): nobody can link the same bidder's bids among different rounds of an auction.

As for privacy, it can be classified into bid privacy and bidder anonymity. Bid privacy: only the winning bid is made public; losing bids should remain the secret [4,8]. Bidder anonymity: the identity of bidders is protected. No one should learn about the identity of losing bidders [4,7].

As an important security problem in online auction, bidder anonymity is studied by researchers [4,7,9-11]. In 2003, Chang and Chang proposed an efficient anonymous auction protocol, which uses encryption to implement bidder anonymity [9]. Later, Jiang et al. proposed an improvement on Chang et al.'s anonymous auction protocols to overcome the security weakness, and they still use encryption to implement bidder anonymity [10]. Xiong et al. proposed an English auction protocol, which comprises three interactive parties: the registration manager, the auction manager and the bidder. It provides conditional privacy-preservation for bidder, only the cooperation of registration manager and auction manager can reveal the identity of a bidder [7]. In 2009, Fan et al. proposed an anonymous rewarding protocol based on electronic cash, which uses anonymous channels to provide message anonymity. Anonymous channels can protect the privacy of a sender against the receiver when the sender submits messages to the receiver, which is based on public-key encryptions [11]. Bidder privacy also led to a series of problems, such as shill bidding.

Fairness is another important security research direction. Xiong et al. mainly use the bulletin board to achieve public verifiability [7]. Palmer proposed a protocol for verification of an auction without revealing bid values, which can be achieved by the use of zero knowledge proofs to verify the auction procedure [12]. In addition, secure multiparty computation was also used to support the fairness of online auction [13].

In this paper, the proposed scheme mainly focuses on bid privacy, bidder anonymity and fairness problem. Although they already proposed some techniques to achieve bidder anonymity [4,7,9-11], there still are security weaknesses. One of the most important problem is the conflict between bidder anonymity and DOS (denial-of-service) attack from insider. We propose a new solution for that. The proposed protocol utilizes ticket token to restrict download; also the market generates deal sequence number (dsn) and random number (r) for suppliers who have downloaded requests for quotes (RFQ). It utilizes efficient LPN-based authentication method to accomplish lightweight authentication. In order to share the determination process data, the market constructs a simple interpolating polynomial to those suppliers who participated in this auction. Sharing the determination process data can totally avoid collusion between a customer and a certain supplier and achieve public verifiability.

Jaiswal et al. proposed a security protocol and put it into real-world networks and analyze security problem to improve MAGNET in 2004 [14]. The proposed major modification is the use of a publish/subscribe system by the market to notify the agents about the auctions. Also, they adopted time-release cryptography to guarantee non-disclosure

of the bids and anonymous communication to hide the identities of the bidders. According to this, the MAGNET is improved in security. The improved protocol still has some weaknesses: vulnerable to the replay data attack, DOS (denial-of-service) attack, anonymity disclosure weakness, collusion between a customer and a certain supplier [15].

In 2003, Chang and Chang proposed an anonymous auction protocol, and they applied a simple method for ensuring anonymity of bidders, and it also provided some important properties of auction protocol [9]. However, Jiang et al. found there were still some weaknesses in the initial phase of Chang et al.'s protocol, so they improved it and proved its security in 2005 [10]. Because computation cost is not taken into account in their improvement, Chang et al. proposed the enhancement with the alias in their protocol and analyzed the computation cost in 2006 [16]. Another protocol was proposed by Liaw et al. in 2006, which provided auction properties. They indicated that their protocol had strong security and more efficient [17]. In 2008, Wu et al. pointed out security drawbacks of Liaw et al.'s protocol and proposed a new online sealed-bid auction scheme which is more efficient and secure than Liaw et al.'s protocol [18]. In 2011, Li et al. proposed a new scheme to resolve Chang et al.'s problems in which two managers and zero knowledge proof are used [4]. By comparative analysis with those protocols, the proposed protocol requires less computation cost.

2. **Security Assumptions.**

As for sealed-bid auction, Shih et al. and Jaiswal et al. proposed their assumptions for that [14,19].

In Shih et al.'s protocol, bid privacy is based on: (1) Auctioneer and the winner do not conspire. (2) Auctioneer and third trusted party do not conspire.

In Jaiswal et al.'s protocol, they proposed some trust assumptions for market as follows. (1) Conveying RFQs from customer to supplier agents. (2) Communicating the bids from supplier agent back to customer agent. (3) Keeping records of all the transactions of RFQs and bids. (4) Aggregating statistical data to ensure non-repudiation. Also, they propose some trust assumptions for three-party as follows. (1) Customer agent will not collude with any of the supplier agents. (2) Customer agent communicates with the supplier agents only through the market.

In the proposed scheme, it follows Jaiswal et al.'s trust assumptions for market and releases the trust assumptions for three-party. Collusion between customers, market and suppliers can not happen in the proposed scheme. Furthermore, the proposed scheme allows the customer agents and the supplier agents to exchange information. This study will introduce how it can relax trust assumptions for three-party and Shih et al.'s assumptions in the later section.

3. **Proposed Architecture.**

3.1. **Key techniques.**

3.1.1. *Ticket token.* For the proposed auction scheme, it requires a secure authentication system for group communication. Also, it requires a mechanism which protect identities of participant in supplier group. So, this study introduces the concept of conference key distribution into the proposed auction scheme. Because of adopting publish/subscribe system, we are going for anonymity primarily, not just for the mutual authentication. In these situations, it is more important that the identities of the suppliers participating in an auction procedure are hidden from other attending suppliers. Furthermore, the participant suppliers should be anonymous to the market and customers.

3.1.2. *LPN-based authentication.* Because this study requires a low-computation and low-storage scheme which is suitable for agents or RFID tags, the proposed scheme introduces the well-proofed Learning parity with noise (LPN) problem. The original LPN problem with security parameters q, k, η. Let A be a random $q * k$ binary matrix, let x be a random k-bit vector, let η be a constant noise parameter, where $\eta \in [0, 1/2]$, and let v be a q-bit vector such that $|v| \leq q$. Given A, η and $z = A \cdot x \oplus v$, find a k-bit vector x' such that $|A \cdot x' \oplus z| \leq q$. The hardness of the computational LPN problem has been shown to be NP-complete [20].

3.2. **Proposed scheme.** The proposed protocol has the following phases: planning, bidding, auction close and winner determination, Figure 1 illustrates the proposed protocol, as explained in the following:

For convenience, this study assumes that there are n_1 customers and n_2 suppliers and the market in the proposed auction scheme. In order to guarantee the reliability and safety among the market, customer group and supplier group, it requires a certification authority (CA) in key pre-distribution process.

CA chooses and publishes large prime number p_1, p_2 such that $p_1 - 1$ and $p_2 - 1$ have large prime factors. Let q_1 be a prime divisor of $p_1 - 1$ and g_1 be a generator with order q_1 in $GF(p_1)$, q_2 be a prime divisor of $p_2 - 1$ and g_2 be a generator with order q_2 in $GF(p_2)$. Let S be the identity of the supplier, C be the identity of the customer. By using the Diffie-Hellman scheme, CA assigns a secret key $x_{i_1} \in Z^*q_1$ and computes public key $y_{i_1} = g_1^{x_{i_1}} \bmod p_1$ for each customer and the market, where $1 \leq i_1 \leq n_1 + 1$. Then, gives the secret key x_{i_1} to each customer and the market in a secure way; CA assigns a secret key $x_{i_2} \in Z^*q_2$ and computes public key $y_{i_2} = g_2^{x_{i_2}} \bmod p_2$ for each supplier and the market, where $1 \leq i_2 \leq n_2 + 1$. Then, CA gives the secret key x_{i_2} to each supplier and the market in a secure way. CA assigns two symmetric key $x_{i_3} \in R\{0,1\}^k$, $y_{i_3} \in R\{0,1\}^k$ for each supplier and the market, where $1 \leq i_3 \leq n_2 + 1$. Then, CA gives the symmetric secret key x_{i_3} and y_{i_3} to each supplier and the market in a secure way.

3.2.1. *Planning.* A customer sends an *RFQ* message which is signed by his secret key S_{k_c} to the market for publishing. After receiving the *RFQ* message, the market verifies and publishes it. After that, The market performs the following steps to construct ticket token polynomial:

1. The market randomly chooses an integer r and a ticket token $T \in Z^*q_2$ and gets a timestamp t from the system and compute $A = g^r \bmod p$, $B = r * T + H(t \parallel A) * x_{m_2} \bmod q_2$, where $H()$ is a one-way hash function.
2. Compute the secret key shared by each supplier as: $k_{m_{i_2}} = y_{i_2}^r \bmod p_2$, where $1 \leq i_2 \leq n_2$.
3. The market constructs ticket token polynomial $f(x)$ for publishing.

$$\begin{aligned} f(x) &= \prod_{i_2=1}^{n_2} (x - k_{m_{i_2}}) + T \bmod p_2 \\ &= x^n + C_{n-1}x^{n-1} + \ldots + C_1 x + C_0 \bmod p_2 \end{aligned}$$

   where $k_{m_{i_2}} = y_{i_2}^r \bmod p_2$ and $C_{n-1}, C_{n-2}, \ldots, C_1, C_0 \in Z^*q_2$.
4. The market publishes A, B, t, C_{n-1}, C_{n-2}, …, C_1, C_0.

3.2.2. *Bidding.* If a supplier S is interested in this auction session, S will

1. Get A, B, t, C_{n-1}, C_{n-2}, …, C_1, C_0 from the market's publish board.
2. Check whether the timestamp t is a valid data or not.
3. Compute the secret key shared with the market as $k_{i_{2_m}} = A_2^{x_i} \bmod p_2$.

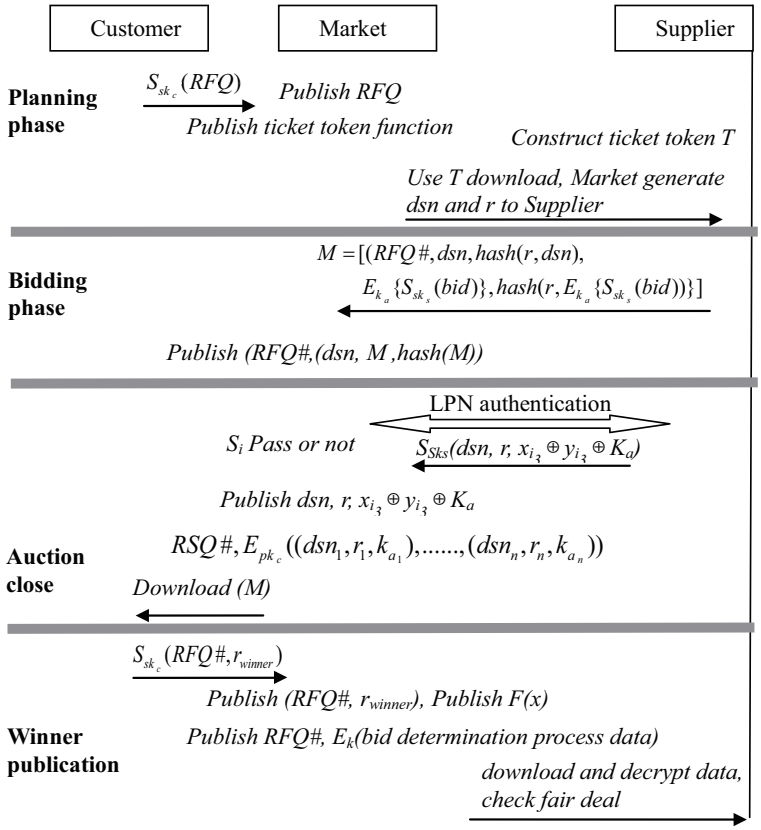

FIGURE 1. The proposed protocol

4. Get ticket token by computing $f(k_{i_{2_m}})$

$$\begin{aligned} f(k_{i_{2_m}}) &= (k_{i_{2_m}})^n + C_{n-1}(k_{i_{2_m}})^{n-1} + \ldots + C_1(k_{i_{2_m}}) + C_0 \bmod p_2 \\ &= T \bmod p_2 \end{aligned}$$

5. Verify ticket token T by computing $H(t \parallel A)$ and check the equation $g^B \equiv A^T * y_{m_2}^{H(t\|A)} \bmod p_2$.

After getting T, the supplier uses the ticket token T to download RFQ. When a legitimate supplier downloads the RFQ, the market generates dsn and r to the supplier. After getting dsn and r from the market, the supplier generates a bid-message comprising of RFQ number ($RFQ\#$), dsn and r, symmetric auction-session key (k_a), bid data (bid). Then he signs, hashes and encrypts the message (M) and sends M to the market, where $M = [RFQ\#, dsn, hash(r, dsn), E_{k_a}(S_{S_{k_s}}(bid)), hash(r, E_{k_a}(S_{S_{k_s}}(bid)))]$, $S_{S_{k_s}}(bid)$ is a bid data block signed by supplier's secret key S_{k_s}. After receiving messages came from suppliers, the market publishes all $(RFQ\#, (dsn, M, hash(M)))$ on the publish board. Suppliers can check and verify whether their own bid-message is actually received and displayed by the market.

3.2.3. *Auction close.* When the auction is closed, the market authenticates supplier's agent by using LPN authentication method.

The two k-bit vectors x_{i_3} and y_{i_3} are secret keys shared by the market and a supplier S, where S denotes identity of the supplier. Figure 2 illustrates one round of our LPN-based authentication.

1. S chooses a blinding vector a_1 randomly, and sends $\{dsn, S, a_1, T_1\}$ to the market, where T_1 denotes a valid timestamp.

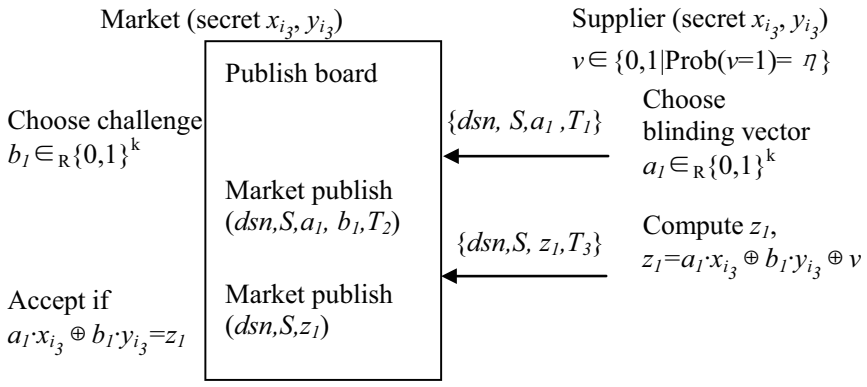

FIGURE 2. One round of LPN-based authentication

2. After receiving $\{dsn, S, a_1, T_1\}$, the market checks T_1 and chooses challenge b_1 randomly, publishes $\{dsn, S, a_1, b_1, T_2\}$, where T_2 denotes a valid timestamp.
3. S gets b_1 from publish board, then computes response $z_1 = a_1 \cdot x_{i_3} \oplus b_1 \cdot y_{i_3} \oplus v$, and sends $\{dsn, S, z_1, T_3\}$, where v denotes a noise bit, T_3 denotes a valid timestamp.
4. After receiving $\{dsn, S, z_1, T_3\}$, the market checks T_3 and publishes $\{dsn, S, z_1\}$ and accepts the round if $a_1 \cdot x_{i_3} \oplus b_1 \cdot y_{i_3} = z_1$.

After that, the market publishes notice which announced whether the supplier's agent passes the authentication or not. If passed, supplier's agent sends $S_{S_{k_s}}(dsn, r, x_{i_3} \oplus y_{i_3} \oplus K_a)$, after receiving it, the market publishes $(dsn, r, x_{i_3} \oplus y_{i_3} \oplus K_a)$. Suppliers can check whether their messages are correctly received and displayed by the market. The market publish $RFQ\#, E_{p_{k_c}}((dsn_1, r_1, k_{a_1}), \ldots, (dsn_i, r_i, k_{a_i}), \ldots, (dsn_n, r_n, k_{a_n}))$, where $E_{p_{k_c}}()$ is encrypted by customer's public key. According to the message which the market published, the customers download corresponding M from the publish/subscribe system and decrypt data block and get all valid bid information. After authenticate supplier group twice, the market can make sure that it would publish valid supplier's information.

3.2.4. *Winner determination.* The customer determines a winner and sends message $S_{S_{k_c}}(RFQ\#, r_{winder})$ to inform the market winner information. After receiving the customer's message, the market checks whether the winner is contained in legal supplier list $(dsn_1, r_1, k_{a_1}), \ldots, (dsn_i, r_i, k_{a_i}), \ldots, (dsn_n, r_n, k_{a_n})$. If the winner is contained in the list, the market publishes the winner information on board for notifying suppliers. If there is a controversy about winner, the market chooses a large prime number p and a primitive element g for $GF(p)$, where $GF(p)$ is the set of integers $\{0, 1, \ldots, p-1\}$ with arithmetic operations defined modulo p. The market generates a symmetric session key K, $K \in Z^*q$. Then the market uses the signature datum of suppliers who participated in current auction to construct a derivation function $F(x)$ and conceals K in it. After that, the market publishes the coefficient $C_{n-1}, C_{n-2}, \ldots, C_1, C_0$ of the $F(x)$, where $S_{S_{k_{s_i}}}(k_{a_i}, r_i)$ are supplier's signature data $(i = 1, 2, \ldots, n)$. The market encrypts bid determination process data and publish $RFQ\#$, E_k (bid determination process data).

$$\begin{aligned} f(x) &= \prod_{i_2=1}^{n_2}(x - h_i) + K \bmod p \\ &= x^n + C_{n-1}x^{n-1} + \ldots + C_1 x + C_0 \bmod p \end{aligned}$$

where $h_i = g^{S_{S_{k_{s_i}}}(k_{a_i}, r_i) \bmod p-1}$ and $C_{n-1}, C_{n-2}, \ldots, C_1, C_0 \in Z^*q$.

4. Security Analysis.

Theorem 4.1. *Assume that no man can modify publish message except the market. After the market publishes* $A = g^r \bmod p$, $B = r * T + H(t \parallel A) * x_{m_2} \bmod q_2$, t, *coefficients* $C_{n-1}, C_{n-2}, \ldots, C_1, C_0 \in Z^* q_2$ *of ticket token function* $f(x) = \prod_{i_2=1}^{n_2} (x - k_{m_{i_2}}) + T \bmod p_2$, *where* $f(x) = x^n + C_{n-1}x^{n-1} + \ldots + C_1 x + C_0 \bmod p_2$, *no man can get ticket token except supplier group.*

Proof: Because the market computes each supplier's secret key $k_{m_{i_2}}$ as the solution of the ticket token polynomial function $f(x)$, where $k_{m_{i_2}} = y_{i_2}^r \bmod p_2$, $1 \le i_2 \le n_2$. Furthermore, only legal suppliers can compute $K_{i_{2_m}} = A^{x_{i_2}} \bmod p_2$, where $k_{m_{i_2}} = k_{i_{2_m}}$. So, legal supplier can have the valid $k_{m_{i_2}}$ that satisfies $f(k_{m_{i_2}}) = T \bmod p_2$ for getting ticket token T.

Situation 1. Obviously, if one attacker wants to obtain r from $A = g^r \bmod p$, he will face the difficulty of solving the intractable discrete logarithm problem [21].

Situation 2. If one attacker wants to obtain T from $B = r * T + H(t \parallel A) * x_{m_2} \bmod q_2$, because there are two unknown parameters r and x_{m_2}, still he must solve the intractable discrete logarithm problem.

Situation 3. If one attacker wants to compute T from the function $f(x)$, he should know the valid $k_{m_{i_2}}$ that satisfies $f(k_{m_{i_2}}) = T \bmod p_2$. Obviously, it means that the attacker must solve the intractable discrete logarithm problem [21].

Because the proposed scheme is sealed-bid auction, it is easy to be attacked by DOS attack from outside malicious impersonator in the bidding phase. By Situations 1-3, only legal suppliers can compute and get factor, construct legal bid. It reduces illegal bid from outsiders, and reduces the possibility of DOS attack from outsiders. Draw a conclusion, the proposed scheme reduces DOS attack from malicious impersonator and keeps anonymity in the planning phase.

Theorem 4.2. *Assume that the market received supplier's message* M_1 *safely, where the message is* $M_1 = [RFQ\#, dsn, hash(R, dsn), E_{k_a}(S_{S_{k_s}}(bid)), hash(R, E_{k_a}(S_{S_{k_s}}(bid)))]$. *The market can make sure that* M_1 *comes from legal supplier group. After the market publishes* $(RFQ\#, (dsn, M_1, hash(M_1)))$ *on board, supplier can make sure that the market received RFQ very well.*

Proof: Suppliers open $RFQ\#$ and dsn information for temporary identity in M_1. We make sure that the key k_a larger than 160 bits, so it is able to withstand the exhaustive key search attack on data block $E_{k_a}(S_{S_{k_s}}(bid))$ [22]. Because the market cannot decrypt the data block $E_{k_a}(S_{S_{k_s}}(bid))$, and the market recorded R as R' in the planning phase, the market can just verify whether information dsn and data block $E_{k_a}(S_{S_{k_s}}(bid))$ are valid by computing $hash(R, dsn)? = hash(R', dsn)$ and $hash(R, E_{k_a}(S_{S_{k_s}}(bid)))? = hash(R', E_{k_a}(S_{S_{k_s}}(bid)))$. After verifying the data block, the market can make sure whether M_1 come from legal supplier or not. After the market published $(RFQ\#, (dsn, M_1, hash(M_1)))$ on board, supplier can verify whether the market receive their message M_1 correctly by computing $hash(M_1)? = hash(M_1')$.

We assume that one attacker cannot get valid R, so the attacker cannot forge valid $hash(R, dsn)$ and $hash(R, E_{k_a}(S_{S_{k_s}}(bid)))$. Furthermore, we assume that the attacker gets valid R, then the attacker forges valid $hash(R, dsn)$ and $hash(R, E_{k_a}(S_{S_{k_s}}(bid)))$. Because of valid $hash(R, dsn)$ and $hash(R, E_{k_a}(S_{S_{k_s}}(bid)))$, the attacker constructs valid bid data M_1 and passes validation made by the market in the bidding phase. By the mutual authentication of Theorem 4.3, the market eliminates illegal bid data in the auction close phase. So the proposed protocol provides forward secrecy.

Theorem 4.3. *Assume that the market finished the communication with supplier by LPN authentication method, then the mutual authentication is achieved between the market and each suppler.*

Proof: The hardness of the computational LPN problem has been shown to be NP-complete [20]. LPN-based authentication method adoptes HB^+ computing prototype in the proposed scheme. Although HB-type protocols are not secure against a man-in-the-middle attack [23], because the proposed auction scheme inherits the idea of the publishing system, so it can make sure that the process of authentication is secure and sets up mutual authentication. Attack of HB^+ protocol occurs on condition that the attacker can manipulate challenges sent by the market during the authentication message exchanges. In the proposed LPN-based authentication process, the market utilizes the publishing system to show messages which suppliers sent. So, suppliers can check whether their messages are correctly received and displayed by the market. We assume that there is an attacker in the middle, and he can manipulate the message sent by a supplier. However, the attacker cannot modify any information, because the supplier can check the message on the board each round. Because of the publishing system, the attacker cannot manipulate the challenges published by the market. According to what is mentioned above, the attacker does not have any opportunity to disturb the authentication process.

Theorem 4.4. *Assume that the market publishes message correctly, where message are coefficients* $C_{n-1}, C_{n-2}, \ldots, C_1, C_0 \in Z^*q$ *of polynomial function* $F(x) = \prod_{i=1}^{n}(x - h_i) + K \bmod p$, *where* $F(x) = x^n + C_{n-1}x^{n-1} + \ldots + C_1x + C_0 \bmod p$ *and* E_k *(bid determination process data), then the market can make sure that suppliers who participated in this auction can check fair deal.*

Proof: Because the market computes each supplier's signature data $S_{S_{k_{s_i}}}(k_{a_i}, R_i)$ as the solution $h_i = g^{S_{S_{k_{s_i}}}(k_{a_i}, r_i) \bmod p-1}$ of the polynomial function $F(x)$, where $S_{S_{k_{s_i}}}(k_{a_i}, R_i)$ is supplier's signature data $(i = 1, 2, \ldots, n)$. So only legal suppliers who participated in this auction session have the valid h_i which satisfies $f(h_i) = K \bmod p$ to compute K from the function. After getting K, each supplier can decrypt data block E_k (bid determination process data) and check the fair deal.

Situation 1. If one attacker wants to compute K from the coefficients of function $F(x)$, he should know the valid $h_i = g^{S_{S_{k_{s_i}}}(k_{a_i}, r_i) \bmod p-1}$ which satisfies $F(h_i) = K \bmod p$. It means that the attacker must solve the intractable discrete logarithm problem [21]. Therefore, the attacker certainly cannot reconstruct the polynomial $F(x)$ to get the session key K from n points $(1, F_i(1)), (2, F_i(2)), \ldots,$ and $(n, F_i(n))$ only. By Theorem 4.1, it is concluded that no one can get ticket token to take part in auction session except supplier group. By Theorem 4.2, it is concluded that the market can make sure that the message which contained bid information comes from legal supplier group, also supplier can check whether the market receives it very well. By Theorem 4.3, it is concluded that the mutual authentication is achieved between the market and each supplier after finished LPN authentication method. By Theorem 4.4, it is concluded that only suppliers who participated this auction session can check fair deal. By the process of winner publication and Theorem 4.4, it is clear that the proposed scheme releases Shih et al.'s assumptions. By the whole procedure and Theorems 4.1-4.4, the proposed scheme releases Jaiswal et al.'s trust assumptions for three-party evidently.

5. **Poperties Achieved and Discussion.** In this section, we discuss the proposed protocol with other protocols. The first comparison is summarized in Table 1 [4,16-18].

There is not a deliberate mechanism which can avoid opening bid before bidding phase is closed in Chang et al.'s protocol. Sealed-bid security is an inherent weakness, because it is not easy to avoid auctioneer opening bids especially in two party's protocol. Chang et al.' protocol provides an opportunity for collusion between an auctioneer and a certain bidder, and the auctioneer leaks bid information to the bidder. In Liaw et al.'s protocol, if the third party tries to open bid data earlier, he also can leak the information to a bidder whom he intend to collude with. Because the proposed protocol can guarantee non-disclosure of a bid, no one except the bidder can access his own bid before the auction close phase.

The anonymity of bidders depends on auctioneers or the third party separately in Chang et al.'s protocol, Liaw et al.'s protocol and Li et al.'s protocol. If auctioneers or the third party intends to collude with a certain bidder, they can break the anonymity of bidders. In the proposed protocol, no one but the bidder himself can open encryption before the bidding phase is closed. This is a way that can guarantee identity non-disclosure independently. Chang et al.'s protocol, Wu et al.'s protocol, Li et al.'s protocol and the proposed protocol utilize signature technique for non-repudiation. Identity can be checked immediately, so it is active manner. Liaw et al.'s protocol uses the random number for non-repudiation, and they must record the data and authenticate identity after an interval. If we do not pursue those data, we cannot know it exactly.

The comparisons of the computation operations of the initial phase and the bidding phase among these protocols are shown in Table 2 [4,16-18]. Assume that the length of the prime number p is 1024 bits in Diffie-Hellman and public key encryption, symmetric key length is 128 bits (for AES) [24], hash function digest is 160 bits (for SHA-1), public key certification is 1024 bits, signature length is 320 bits (for DSA). Because RSA's computation operation can be summarized as a modular exponentiation operation, and the computation operation of a modular exponentiation is about $O(\mid n \mid)$ times that of a modular multiplication, where $\mid n \mid$ denotes the bit length of n. So compared with a modular multiplication computation in Z_n^*, the computation time consumed by hashing operations, symmetric encryptions or decryptions can be neglected [25]. Symmetric cryptosystem is faster 1000 times than asymmetric cryptosystem and hash function is faster 10 times than symmetric cryptosystem [18,26].

Although liaw's protocol excludes all the computation operations of bank party, it is still more inefficient than Chang's protocol. According to Table 2, it is observed that the proposed scheme's total numbers of modular exponentiation computations are less

Table 1. The achieved properties

Properties	Chang [16]	Liaw [17]	Wu [18]	Li [4]	Proposal
Using timestamp	Yes	No	Yes	Yes	Yes
Using symmetric key	Yes	No	Yes	Yes	Yes
There is a trusted third-party	No	Yes	Yes	Yes	Yes
Can open bid before auction closing	Yes	Yes	No	No	No
Anonymity	Dependently	Dependently	No	Dependently	Independently
The number of parties	2	4	4	4	3
Non-repudiation	Actively	Passively	Actively	Actively	Actively

TABLE 2. The numbers of different computation operations

Phase	Chang [16]	Liaw [17]	Wu [18]	Li [4]	Proposal
The initiation phase	4 HF	5 HF	3 HF	0	2 HF
	2 SKE	0	2 SKE	0	0
	2 SKD	0	0	0	0
	2 PKE	3 PKE	0	3 PKE	1 PKE
	2 PKD	3 PKD	0	0	1 PKD
	4 ME	0	2 ME	5 ME	4 ME
	2 R	5 R	0	0	5 R
The bidding phase	0	0	0	1 HF	4 HF
	2 SKE	0	0	1 SKE	1 SKE
	2 SKD	0	0	0	0
	1 PKE	5 PKE	0	1 PKE	1 PKE
	1 PKD	5 PKD	0	0	0
	0	0	4 ME	0	0

PKE: Public Key Encryption; PKD: Public Key Decryption; SKE: Symmetric Key Encryption; SKD: Symmetric key decryption; HF: Hash Function; ME: Modular Exponentiation; R: generate a random number

than those of Wu's protocol and Li's protocol. Obviously, the proposed protocol is more efficient than other protocols in total.

6. **Conclusions.** As mentioned above, the current paper demonstrated that the proposed electronic marketplace bidding auction protocol protects bidder anonymity and bid privacy, and avoids collusion among parties. Also, it satisfies the security requirements of an electronic auction, such as anonymity, non-repudiation, verifiability. The proposed scheme relaxes some trust assumptions for three-party in Jaiswal's scheme. According to the discussion and analysis with Chang et al.'s protocol and Liaw et al.'s protocol, the proposed protocol requires less computation cost in the initiation phase and the bidding phase, and has better security in anonymity, fairness and reliance on the third party. Therefore, the proposed bidding auction protocol's advantage is that collusion occurs difficultly and computation cost is low.

REFERENCES

[1] L. I. de Castro and D. H. Karney, Equilibria existence and characterization in auctions: Achievements and open questions, *Journal of Economic Surveys*, 2011.

[2] C.-C. Lina, S.-C. Chenb and Y.-M. Chu, Automatic price negotiation on the web: An agent-based web application using fuzzy expert system, *Expert Systems with Applications*, vol.38, no.5, pp.5090-5100, 2011.

[3] A. H. Ozer and C. Ozturan, Multi-unit differential auction-barter model for electronic marketplaces, *Electronic Commerce Research and Applications*, vol.10, pp.132-143, 2011.

[4] M.-J. Li, J. S.-T. Juan and J. H.-C. Tsai, Practical electronic auction scheme with strong anonymity and bidding privacy, *Information Sciences*, vol.181, no.12, pp.2576-2586, 2011.

[5] K. Omote and A. Miyaji, A practical English auction with one-time registration, *Lecture Notes in Computer Science*, vol.2119, pp.221-234, 2001.

[6] Y.-F. Chung, Y.-T. Chen, T.-L. Chen and T.-S. Chen, An agent-based English auction protocol using elliptic curve cryptosystem for mobile commerce, *Expert Systems with Applications*, vol.38, pp.9900-9907, 2011.

[7] H. Xiong, Z. Chen and F. Li, Bidder-anonymous English auction protocol based on revocable ring signature, *Expert Systems with Applications*, vol.39, pp.7062-7066, 2012.

[8] W. Shi and W. Wei, An improved efficient electronic marketplace bidding auction protocol with bid privacy, *Journal of Convergence Information Technology*, vol.6, no.2, pp.272-282, 2011.
[9] C. C. Chang and Y. F. Chang, Efficient anonymous auction protocols with freewheeling bids, *Computer & Security*, vol.22, no.8, pp.728-734, 2003.
[10] R. Jiang, L. Pan and J. H. Li, An improvement on efficient anonymous auction protocols, *Computer & Security*, vol.24, no.2, pp.169-174, 2005.
[11] C.-I Fan, S.-Y. Huang, P.-H. Ho and C.-L. Lei, Fair anonymous rewarding based on electronic cash, *Journal of Systems and Software*, vol.82, no.7, pp.1168-1176, 2009.
[12] B. Palmer, K. Bubendorfera and I. Welch, A protocol for verification of an auction without revealing bid values, *Procedia Computer Science*, vol.1, no.1, pp.2649-2658, 2010.
[13] M. Hinkelmann, A. Jakoby, N. Moebius, T. Rompf and P. Stechert, A cryptographically t-private auction system, *Concurrency and Computation: Practice and Experience*, vol.23, no.12, pp.1399-1413, 2011.
[14] A. Jaiswal, Y. Kim and M. Gini, Design and implementation of a secure multi-agent marketplace, *Electronic Commerce Research and Applications*, vol.3, no.4, pp.355-368, 2004.
[15] W. Shi, I. Jang and H. S. Yoo, An efficient electronic marketplace bidding auction protocol with bid privacy, *Lecture Notes in Computer Science*, vol.4976, pp.297-308, 2008.
[16] Y. F. Chang and C. C. Chang, Enhanced anonymous auction protocols with freewheeling bids, *Proc. of the 20th International Conference on Advanced Information Networking and Applications*, vol.1, pp.353-358, 2006.
[17] H.-T. Liaw, W.-S. Juang and C.-K. Lin, An electronic online bidding auction protocol with both security and efficiency, *Applied Mathematics and Computation*, vol.174, no.2, pp.1487-1497, 2006.
[18] C.-C. Wu, C.-C. Chang and I.-C. Lin, New sealed-bid electronic auction with fairness, security and efficiency, *Journal of Computer Science and Technology*, vol.23, no.2, pp.253-264, 2008.
[19] D.-H. Shih, B. Lin and S.-Y. Huang, MoRVAM: A reverse Vickrey auction system for mobile commerce, *Expert Systems with Applications*, vol.32, no.4, pp.1113-1123, 2007.
[20] K. Pietrzak, Cryptography from learning parity with noise, *SOFSEM 2012: Theory and Practice of Computer Science, Lecture Notes in Computer Science*, vol.147, pp.99-114, 2012.
[21] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, 1st Edition, Springer, 2001.
[22] National Institute of Standards and Technology (NIST), Digital signature standard, *Federal Information Processing Standards Publication, FIPS PUB 186*, p.20, 1994.
[23] E. Kiltz, K. Pietrzak, D. Cash, A. Jain and D. Venturi, Efficient authentication from hard learning problems, *Advances in Cryptology-Eurocrypt 2011, Lecture Notes in Computer Science*, vol.6632, pp.7-26, 2011.
[24] Y.-S. Yeh, C.-Y. Lee, T.-Y. Huang and C.-H. Lin, A transpositional advanced encryption standard (AES) resists 3-round square attack, *International Journal of Innovative Computing, Information and Control*, vol.5, no.5, pp.1253-1264, 2009.
[25] C.-I Fan, Y.-C. Chan and Z.-K. Zhang, Robust remote authentication scheme with smart cards, *Computers & Security*, vol.24, no.8, pp.619-628, 2005.
[26] C. C. Chang, C. S. Lail and L. Harn, *Contemporary Cryptography and Its Applications*, 2nd Edition, Unalis Co, 2001.